A publication of the DCIS Northeast Field Office

TECHNOBABBLE

The DCIS Cyber Crime Newsletter

TECHNOBABBLE
Volume 2, Issue 6

November, 2001

This issues suggested computer crime bookmarks:

Cybercrimes.net's Terrorism Page

http://cybercrimes.net/Terrorism/terrorism.html

Cyberterrorism Position Papers

http://www.isu.edu/gost/cctws/positions.html

Google's Cyber Terrorism Directory :

http://directory.google.com/Top/Society/Issues/Terrorism/Cyber_Terrorism/

Inside this issue:

The Cyberterrorism Threat: All Too Real

The tragic events of September 11, 2001, have forced the nation to reevaluate its stance on issues relating to security, including potential threats involving cyber attacks. On October 17, 2001, Virginia Governor James Gilmore addressed Congress relative to the impending threat of a terrorist related electronic strike.

"Prior to September 11, many people questioned whether nation states or rogue terrorists had the capability to disrupt our critical infrastructures on a wide scale. Since September 11, we must presume they *do,*" stated Gilmore.

Gilmore currently serves as Chairman of a panel created by Congress in 1998 to assess the capabilities for domestic response to terrorism involving weapons of mass destruction. The panel has repeatedly stressed the importance of securing the nation's information infrastructure from potential attack.

According to Gilmore, "critical information and communication infrastructures are targets for terrorists because of the broad economic and operational consequences a shutdown can inflict." Gilmore went on to say, "our banking and finance systems, our "just-in-time" delivery systems for goods, our hospitals, our state and local emergency services… all of these critical services rely upon their information connections and databases to… each is critical to the American economy and health of our citizens, and each can be shut down or severely handicapped by a cyber attack."

Gilmore pointed out the fact that the economic, telecommunication, and infrastructure disruptions caused by the airplane crashes of September 11 were mere collateral impacts upon the information technology sector, and noted that the impacts of a direct assault upon the IT infrastructure could prove disastrous. "We need only to look at the consequences of cyber-hackers and recent viruses like Code Red and Nimda to contemplate the severe economic and governmental harm that could be inflicted."

Some of the specific recommendations presented to Congress include the following:

· The development of a "top to bottom" national approach to dealing with potential cyber security issues, which involves federal, state, and local agencies as well as private sector cooperation.

· Creation of a Congressional panel which specifically focuses upon cyber security, and presents recommendations to the President and Congress.

· Sharing of intelligence and real time information with the private sector through creation of a not-for-profit entity that can represent the interests of both public and private organizations.

· Establishment of a special "Cyber Court" patterned after the court established by the Foreign Intelligence Surveillance Act (FISA) in order to promote effective procedures and understanding of technical issues within the judiciary branch.

· Implemenation of research and development programs to focus specifically on cyber security.

· Conversion of government "Y2K" offices into permanent "cyber security" offices.

For the full text of Governor Gilmore's statements, visit:

www.house.gov/science/full/oct17/gilmore.htm

NIPC Says Cyber Protest Threats will Increase

According to a new Executive Summary issued by the National Infrastructure Protection Center (NIPC), cyber protesting and hacktivism will become more relevant to U.S. interests in the future.

According to the NIPC report, "events and emerging international situations will increasingly lead to cyber protests. The cyber protests that have occurred thus far have had little impact on U.S. infrastructure. As computing technology becomes faster and better, and hacking tools become more advanced and easier to use, cyber protesting and hacktivism will become more significant. Cyber protesters are becoming increasingly more organized and their techniques more sophisticated but, most likely, will continue to deface web sites and perform Denial of Service attacks. There will also be an increase in the number of apparently unrelated hacking groups participating in the cyber protests. National boundaries will not always be clearly delineated in attacks on opposing organizations. International activity will also tend to spill over into the United States. Because the United States is a multicultural, world-leading nation it will suffer from attacks on culturally related sites and structures in the future."

According to the report, the systems which are most attractive to cyber protesters are those of government, educational, commercial, and cultural institutions. However, history has shown that any site with a known vulnerability can become a target. According to the report, "web sites that remain open to known hacking tools will have a higher probability of suffering defacement. Network administrators must remain educated and defenses must evolve along with the threats and offensive capabilities. Although the cyber protests seen today have already caused limited damage, the potential for future attacks could bring about large economic losses as well as potentially severe damage to the national infrastructure, affecting global markets as well as public safety."

What is a Cyber Protest?

Since its' inception, the open nature of the Internet has created an attractive forum for exchange of political views. In our modern era, periods of intense political activity oftentimes results in an increase in on-line political related movements. Unfortunately, various parties are not satisfied in posting political views to publicly accessible Internet news groups, or on their own personal websites. Some individuals seek to attract attention by taking advantage of vulnerabilities which exist on other entities' computers in order to deface the sites, and replace sites' original content with statements relating to their political and ideological views. Others will choose to launch a Denial of Service attack against entities which hold views inconsistent with their own, and will label the attack as a form of protest. Politically motivated computer crime of the nature referenced is oftentimes referred to as "Cyber Protesting," or "hacktivism." Hacktivism proves especially attractive to foreign parties which intend to draw attention to their causes, since these parties can do so via a remote location. The low cost of launching a hacktivism campaign, and relative lack of expertise necessary, make hacktivism especially appealing to protesters with limited budgets and resources.

The Risk

To date, while cyber protesters have been somewhat successful in bringing attention to their causes via hacktivism campaigns, the financial impact upon the IT community has been relatively limited. Systems Administrators generally have backups available of website data, and simply patch their systems and restore from a backup, or configure their routers to block Denial of Service attacks originating from specific IP addresses. However, according to NIPC, this may change. According to the agency's report, "while the cyber damage thus far has been minimal, the infrastructure will certainly be a target of cyber protestors and hacktivists in the future, with the potential goal being intentional destruction rather than public embarrassment or purely political statements. Pro-active network defense and security management are imperative to the prevention of more serious damage to infrastructure assets. International cooperation and private–public cooperation within the United States is necessary to ensure the ongoing function of the critical infrastructure."

"Pro-active network defense and security management are imperative to the prevention of more serious damage to infrastructure assets."

Know the Code!

Common Federal Statutes Utilized in Prosecuting Computer Crime

By Special Agent Jim Ives, DCIS Boston Resident Agency

18 USC 1362—Communication Lines, Stations, or Systems

This issues 'commonly utilized statute' is 18 USC 1362, entitled "Communication Lines, Stations, or Systems." The statute is of special significance to U.S. Department of Defense investigations, as well as investigations involving critical government communication systems.

"Prosecutors faced with instances whereby networks have been compromised by individuals seeking to impair communications (or who inadvertently impair communications via their actions) can utilize this statute as a potential charge."

The following language defines offenses covered by the statute:

Whoever willfully or maliciously injures or destroys or attempts willfully or maliciously to injure or destroy any of the works, property, or material of any radio, telegraph, telephone or cable, line, station, or system, or other means of communication, operated or controlled by the United States, or used or intended to be used for military or civil defense functions of the United States, whether constructed or in process of construction, or willfully or maliciously interferes in any way with the working or use of any such line, or system, or willfully or maliciously obstructs, hinders, or delays the transmission of any communication over any such line, or system, shall be fined under this title or imprisoned not more than ten years, or both.

In the case of any works, property, or material, not operated or controlled by the United States, this section shall not apply to any lawful strike activity, or other lawful concerted activities for the purposes of collective bargaining or other mutual aid and protection which do not injure or destroy any line or system used or intended to be used
for the military or civil defense functions of the United States.

Violators of this statute are eligible to receive sentences of 3 to 10 years in prison, and fines ranging from $1,000 to $10,000.

A brief review of the statute reveals it's original intent—namely, to protect the integrity of communication systems utilized by military and civil defense agencies. Of course, when Congress first drafted this language in 1961, they were most likely interested in prosecuting individuals who **physically** tampered with the systems outlined within the chapter. It is unlikely that Congress could foresee the danger of **remote** computer network attacks being launched against critical information systems by individuals seeking to impair communications between government entities. Fortunately, the broad based language utilized within the statute have helped it stand the test of time. Prosecutors faced with instances whereby networks have been compromised by individuals seeking to impair communications (or who inadvertently impair communications via their actions) can utilize this statute as a potential charge.

It does not take a great deal of consideration to imagine scenarios in which this statute could be utilized. Obviously, if an individual were to hack into a Defense related computer system with the intent of impeding communication between military entities, the statute could be utilized. But the statute could also be utilized in instances whereby a hacker with less of a malicious intent (i.e. a "recreational" hacker) broke into a DoD system on a whim, yet inadvertently crashed the network mail server. Since the hackers actions were still malicious in nature, the statute could be applied. To take this theory a step further, a hacker who invades a government system, yet causes no apparent damage, could also be prosecuted via the statute if prosecutors can establish that the individual's action "obstructs, hinders, or delays the transmission of any communication." One could argue that the mere presence of a hacker on a sensitive communication system will, in fact, delay transmissions by virtue of the fact that every computer network has a limited amount of available bandwidth. If the individual utilizes classic hacker methodology, and establishes a sniffer on the network in question, one could undoubtedly argue that the normal flow of communication has been interfered with (although in this case, prosecutors may wish to use statutes relating to illegal wiretaps, which can carry even harsher penalties). In fact, with a bit of constructive thought, there are very few instances involving surreptitious access to sensitive Defense related systems whereby a prosecutor could not apply the referenced statute.

This Issues Suggested Reading

Cyberwar 2.0: Myths, Mysteries and Reality

The information age confronts us with a new and troubling definition of war and warfare. Those who fight, what they fight about, the weapons they wield, the targets they choose, the rules of engagement, the laws, ethics and mores that govern human behavior in conflict have changed. This is a book about the struggle for the new coin of the realm-information.

Noteworthy is the fact that the editorial review of this book indicates that it is used as a text at the National Defense University, the Joint Military Intelligence Agency and other military institutions.

A recent Amazon.com review states,

"This sequel to the first book on cyberwar is even better (and the first one was very good) because it is much more deliberate about addressing strategy and diplomacy (part one); society, law, and commerce (part two); operations and information warfare (part three, where most military professionals get stuck); and intelligence, assessment, and modeling (part four)."

Title:

Cyberwar 2.0
Myths, Mysteries & Reality

Authors:

Allen Campen & Douglas Dearth

Cost:

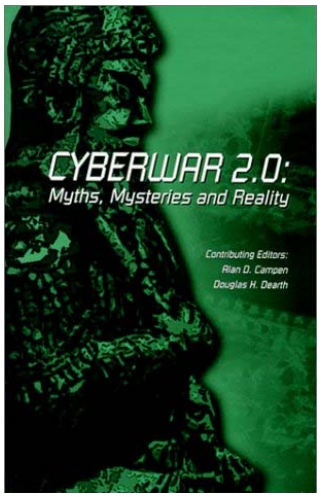
$29.95

ISBN:

0916159272

Publisher:

AFCEA International Press



Bush Panel to Fight Cyberterror

Reprinted from Federal Computer Week, October 17, 2001
By Christopher P. Dorobek

President Bush, calling the protection of information systems critical to the nation's well-being, issued an executive order creating a panel to fight cyberterrorism.

The President's Critical Infrastructure Board has the task of preventing disruptions of the nation's critical infrastructures, Bush said in an executive order issued Oct. 16. Critical infrastructures include such things as transportation and electrical power.

Protecting the networks is vital to protecting "the people, economy, essential human and government services and national security of the United States," Bush said.

The board is responsible for coordinating federal efforts to protect information systems, the executive order says.

In addition to creating the board itself, the executive order puts the director of the Office of Management and Budget in charge of implementing government wide policies, standards and guidelines for protecting federal agency information systems.

The president notes that agencies are "responsible and accountable for providing and maintaining adequate levels of security for information systems, including emergency preparedness communications systems.

"Cost-effective security shall be built into and made an integral part of government information systems, especially those critical systems that support the national security and other essential government programs. Additionally, security should enable, and not unnecessarily impede, department and agency business operations," the executive order says.

A key task of the board will be coordinating efforts with industry, which runs many of the nation's information networks that support critical infrastructures.

The board will be made up of Bush administration Cabinet members, along with many other top presidential aides.

Cybersecurity called Key to Homeland Defense

Reprinted from Federal Computer Week, October 1, 2001
By Diane Frank, with contributions by Dan Caterinicchia

As the Office of Homeland Security takes shape, federal and private-sector technology experts are urging the Bush administration to ensure that cybersecurity is included.

President Bush created the office last month in response to the Sept. 11 terrorist attacks and named Pennsylvania Gov. Tom Ridge as its head. The Cabinet-level office will coordinate, not replace, the many federal, state and local agencies involved in protecting the nation against terrorist attacks, officials said.

"The key here, when it comes to homeland defense, is to have one very effective person at the pinnacle of it who can help coordinate it," White House spokesman Ari Fleischer said last month.

The administration is still determining the office's exact structure, including staffing and funding, Fleischer said. Several bills are moving through Congress to better define the office.
But while much of the reaction to the terrorist attacks has focused on physical security, such as airport and building security, information technology and cybersecurity also must be included, experts said.

"It is likely that a separate strategy will be needed to ensure that critical computer systems are also protected," Joel Willemssen, managing director of IT issues at the General Accounting Office, testified at a hearing last month. "However, it will be essential to link the government's strategy for combating computer-based attacks to the national strategy for combating terrorism."

White House officials have been reviewing the national plan for protecting the country's critical infrastructures, including the telecommunications sector, since January. Now, officials are discussing how that strategy will relate to the Office of Homeland Security, Willemssen said.

The government's lead agency for responding to cyberattacks, the National Infrastructure Protection Center, is helping the investigation. The NIPC also offers vital support to the new office because it coordinates protection and response across different entities, NIPC Director Ronald Dick said.

The coordination between physical and cyber protection is essential as agencies consider what could have happened if the "Nimda" worm, which spread rapidly to affect the Internet, had hit Sept. 11 instead of a week later, experts said.

Intelligence and information sharing among agencies, as well as quick dissemination of information via the Internet, will be crucial to the office's success, said Mark DeMier, deputy director for operations at the Anser Institute for Homeland Security.

"It's going to be essential [because] after the attacks, the Internet was the most reliable way to communicate," he said.
Both high- and low-grade technology will play important roles in helping the new security office do its job, DeMier noted. Everything from facial recognition to air-purification masks should be used, he said.

The Homeland Security Office's effectiveness will depend on Congress' willingness to give agencies adequate resources for any new responsibilities to support the office, said Michael Vatis, director of the Dartmouth College Institute of Security Technology Studies and former NIPC director.
One reason why critical information systems lack adequate security is that many agencies are required to secure the systems without being given the funds to do so, he said.

"Intelligence and information sharing among agencies, as well as quick dissemination of information via the Internet, will be crucial to the office's success…"

CERT Releases Latest Security Statistics

Carnegie Mellon University's CERT team has released their most recent statistics relative to computer security incidents reported to the institution. According to the statistics, although the year is only three-quarters complete, we have already surpassed last years statistics by a significant margin.

Highlights of the statistics reported by CERT are as follows:

· According to CERT, 34,754 incidents have been reported throughout the first three quarters of 2001. Compare this to 21,756 incidents that were reported in 2000.

· 1,820 separate system vulnerabilities were reported in the first three quarters of 2001, compared to a total of 1,090 vulnerabilities which were reported in 2000.

· 29 security alerts have been released by CERT within the first three quarters of 2001, versus 26 reported throughout 2000.

· CERT issued 260 security notes during the first three quarters of 2001, versus 57 issued in 2000.

· CERT received 85,334 separate e-mails throughout the first three quarters of 2001, versus 56,365 received in 2000

A publication of the DCIS Northeast Field Office

Defense Criminal Investigative Service
Northeast Field Office
10 Industrial Highway, Bldg. G, Mail Stop 75
Lester, PA 19113

Phone: (610) 595-1900
Fax: (610) 595-1934

Send comments to: Jives@dodig.osd.mil

We're on the Web!
www.dodig.osd.mil/dcis/dcismain.html

The Defense Criminal Investigative Service

"Protecting America's Warfighters"

The Defense Criminal Investigative Service is the investigative arm of the U.S. Department of Defense, Office of the Inspector General. As such, DCIS investigates criminal, civil, and administrative violations impacting the Defense Department. Typically, DCIS investigations focus upon computer crime involving U.S. military and civilian DoD systems, contract procurement fraud, bribery and corruption, health care fraud, anti-trust investigations, significant thefts of government property, export enforcement violations, environmental violations, and other issues that impact the integrity and effectiveness of the U.S. Department of Defense.

If you encounter issues that impact the U.S. Department of Defense, please call the DCIS office within your region.

DCIS Northeast Field Office.
10 Industrial Hwy., Bldg. G
Lester, PA 19113
Phone: (610) 595-1900
Fax: (610) 595-1934

DCIS Boston Resident Agency
Rm. 327, 495 Summer Street
Boston, MA 02210
Phone: (617) 753-3044
Fax: (617) 753-4284

DCIS Hartford Resident Agency
525 Brook Street, Suite 205
Rocky Hill, CT 06067
Phone: (860) 721-7751
Fax: (860) 721-6327

DCIS New Jersey Resident Agency
Wick Plaza 1, 100 Dey Pl., Ste. 102
Edison, NJ 08817
Phone: (732) 819-8455
Fax: (732) 819-9430

DCIS New York Resident Agency
One Huntington Quad, Suite 2C01
Melville, NY 11747
Phone: (516) 420-4302
Fax: (516) 420-4316

DCIS Pittsburgh Post of Duty
1000 Liberty Ave., Ste. 1310
Pittsburgh, PA 15222
Phone: (412) 395-6931
Fax: (412) 395-4557

DCIS Syracuse Resident Agency
441 S. Selina St., Ste. 304
Syracuse, NY 13202
Phone: (315) 423-5019
Fax: (315) 423-5099